IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF NEW YORK

UNITED STATES OF AMERICA,

v. 21-CR-7-LJV

JOHN STUART,

Defendant.

GOVERNMENT'S RESPONSE TO DEFENDANT'S OBJECTIONS TO THE REPORT, RECOMMENDATION, AND ORDER OF UNITED STATES MAGISTRATE JUDGE JEREMIAH J. McCARTHY

THE UNITED STATES OF AMERICA, by and through its attorneys, Trini E. Ross, United States Attorney, and Laura A. Higgins, Assistant United States Attorney, of counsel, hereby files its response opposing defendant John Stuart's objections (Doc. 36), to the Magistrate Judge Jeremiah J. McCarthy's December 15, 2021 Report and Recommendation, (Doc. 33). The objections should be denied and the Report and Recommendation adopted in its entirety.

I. PROCEDURAL HISTORY

On October 20, 2020, the defendant was charged by Criminal Complaint with violations of 18 U.S.C. §§ 2252A(a)(5)(B) and 2252A(b)(2)(possession of child pornography); 18 U.S.C. §§ 922(g)(3) and 924(a)(2)(unlawful user of controlled substance in possession of a firearm); and 18 U.S.C. § 841(a)(1) and 841(b)(1)(D)(manufacture of marijuana). *See* Doc. 1. On January 20, 2021, the defendant was charged by Indictment with violations of 18 U.S.C. §§ 2252(a)(2)(A) and 2252A(b)(1)(receipt of child pornography); 18 U.S.C. §§ 2252A(a)(5)(B) and 2252A(b)(2)(possession of child pornography); 18 U.S.C. §§ 922(g)(3) and

924(a)(2)(unlawful user of controlled substance in possession of a firearm); and 18 U.S.C. § 841(a)(1) and 841(b)(1)(D)(manufacture of marijuana). *See* Doc. 8.

On October 4, 2021, the defendant filed a pretrial omnibus motion seeking suppression of evidence seized pursuant to a search warrant executed at the defendant's residence on October 19, 2020. *See* Doc. 27. The government responded in opposition, Doc. 28, and oral argument was held before the Honorable Jeremiah J. McCarthy, United States Magistrate Judge, on November 17, 2021. *See* Doc. 32.

On December 15, 2021, Magistrate Judge McCarthy issued a Report and Recommendation recommending this Court deny the defendant's motion to suppress suppress evidence. *See* Doc. 33. In summary, the Magistrate Court found (1) the information relied upon by the affiant on the search warrant application was reliable, (2) the information offered in the search warrant application was not stale, and (3) even if it was stale, the good faith exception would apply. *Id*. The government maintains Magistrate Court correctly decided the issues raised by the defendant and the Court should deny the defendant's motion to suppress.

The Defendant's Objection to the Report and Recommendation

On January 31, 2022, the defendant filed an objection to the Magistrate Court's Report and Recommendation and, for the first time, offered an affidavit from Gerald Grant, a digital forensics expert, stating that "a simple click on [Tor Browser] links can take the user to the hidden website, just as is commonly done on the public internet," and "it is possible for a user to easily find a list of links to hidden Tor websites, click on a link, and be taken to that website without being aware of what content it contains." *See* Doc. 36-1 at ¶¶ 5-6.

The government objects to the defendant's late-stage submission of Gerald Grant's affidavit. Presumably the defendant offers it to create a material issue of fact to dispute statements made and inferences offered by Task Force Officer Michael Hockwater in his search warrant application. Defense counsel, however, surely realized the submission of this affidavit was in violation of Local Rule 59 and the Magistrate Court's reminder that "the district judge will ordinarily refuse to consider…evidentiary material which could have been, but [was] not, presented to the magistrate judge in the first instance." *See* Doc. 33 (*citing Patterson-Leitch Co. v. Massachusetts Municipal Wholesale Electric Co.*, 840 F.2d 985, 990-91 (1st Cir. 1988). Indeed, the defense omitted a certification that his "objections do not raise new legal/factual actuments, or identifying the new arguments and explaining why they were not raised to the Magistrate Judge" as required by Local Rule 59(c)(3). *See* Doc. 36. Even more, the defense offered no explanation as to why the affidavit or its substance was not raised to the Magistrate Court.

Notwithstanding the defense's failure to comply with the Local Rules of Criminal Procedure and the Magistrate Court's reminder, the government is not asking this Court to refuse to consider the defendant's objection altogether. Rather, the government moves to strike Gerald Grant's affidavit and asks this Court to refuse to consider it. The affidavit was prepared and submitted to this Court by the defense 12 months after the government turned over a copy of the search warrant at issue at the time the Indictment was filed, and more than 18 months after the defendant was first charged. Indeed, after the government turned over the search warrant application to the defense in January 2021, it indulged five adjournment motions to extend the time for defense counsel to prepare pretrial motions by the defendant (from April 26, 2021 until October 4, 2021 when the motions were filed). *See* Docs. 16, 18,

20, 23, 25. The defense has offered the Court no reason this affidavit, prepared by its own retained forensic expert, was not prepared and submitted to the Magistrate Court in the first instance in October 2021.

II. STATEMENT OF FACTS

This FBI investigation began as a lead from a national investigation, which received information from international law enforcement partners who dismantled several child pornography sites on the Tor network, often referred to as the "dark web" where users can visit anonymously. During the June 2019 operation, international law enforcement captured the IP addresses of visitors on the dismantled sites. These IP addresses were disseminated to the respective countries and, in the United States, to the districts with venue to prosecute. One such IP address was registered to 1010 Cleveland Drive, Cheektowaga, New York. The information provided by the lead from international law enforcement included the name of the website, a description of it as a "child pornography bulletin board and website dedicated to the advertisement and distribution of child pornography and the discussion of matters pertinent to the sexual abuse of children." The lead also detailed that the website was in operation from approximately October 2016 through June 2019, was located outside of the United States, was seized by the foreign law enforcement authority, and the IP address registered to Stuart's residence was on the site on a particular date and time. Details of the content were verified by the FBI while the site was in operation, which confirmed details about the site including its self-described purpose to "share cp of babies and toddlers," how the site functioned to allow users to make and view postings that contained text, images, video images, and web links directing users to specific content at other websites. FBI Special Agents

accessed the site and downloaded digital child pornography content accessible via the website in an undercover capacity.

The June 2019 lead regarding Stuart's IP address at his residence was transmitted to FBI Buffalo in July 2020. Shortly thereafter, the government obtained authorization to use a pen register and trap and trace device (PRTT) on the target broadband account registered at 1010 Cleveland Drive, Cheektowaga, New York. The PRTT monitored the IP activity on the defendant's residence between August and October 2020. The result of the PRTT confirmed an occupant of the residence was utilizing an internet-connected device to frequent the Tor network, and therefore likely the same type of dark web child pornography sites as what was dismantled in 2019.

A federal search warrant was obtained on October 8, 2020 from the Honorable Michael J. Roemer for the residence at 1010 Cleveland. *See* 20-MJ-5207.[1] The search warrant authorized the seizure and subsequent search of the contents of electronic devices.

The search warrant was executed on October 19, 2020. During the search, law enforcement seized:

- 6 electronic devices: an Apple MacBook, a Samsung cellphone, two Western Digital External Hard Drives, a Dell laptop, and a deskop computer tower
- a grow operation inside the residence which consisted of a tent housing approximately 5 mature marijuana plants, 4 smaller plants, all being grown hydroponically.
- approximately one pound of dried marijuana ready for use
- another quantity of approximately 6 pounds of wet marijuana was located (apparently this will produce approximately 1 pound of marijuana once dried)
- Psilocybin mushrooms were also seized (a Schedule I controlled substance)
- 3 firearms: a Glock model 43X, 9 millimeter pistol bearing serial number BNGY234 loaded with 9 rounds of ammunition (this firearm is registered to Stuart on his NYS pistol permit)

[1] The government has supplied a copy of this application to the defendant and now supplies a copy under separate cover to the Court for *in camera* review.

Stuart was interviewed by an investigator in the defendant's bedroom and the entire interview was recorded on the body camera of a Cheektowaga PD officer. During the interview, the defendant made significant admissions the government intends to use against him at trial.

III. STANDARD OF REVIEW

Title 28, United States Code, Section 636(b)(1)(A) enables the Magistrate Court, upon referral, to adjudicate non-dispositive matters, that is, "any matter that does not dispose of a charge or defense." See Fed. R. Crim. P. Rule 59(a). This Court may reconsider orders of the Magistrate Court on such matters "where it has been shown that the magistrate judge's order is clearly erroneous or contrary to law." See § 636(b)(1)(A). Under Local Rule 59(c)(1), "[t]he specific matters to which the party objects and the manner in which it is claimed that the order is clearly erroneous or contrary to law shall be clearly set out in the objections."

Title 28, United States Code, Section 636(b)(1)(B) enables the Magistrate Court, upon referral, to conduct hearings and submit to this Court proposed findings of fact and recommendations of law for dispositive matters, including motions to suppress evidence. The same section requires the District Court to make a *de novo* determination of those portions of the report or specified proposed findings or recommendations to which objection is made. A judge of the court may accept, or modify, in whole or in part, the finding or recommendations made by the magistrate. The judge may also receive further evidence or recommit the matter to the magistrate with instructions. See § 636(b)(1)(C). In making its independent determination, "[i]t is sufficient that the district court 'arrive at its own, independent conclusion about those portions of the magistrate's report to which objection is made . . . .' To this end, the court must 'exercise . . . sound judicial discretion with respect to whether

reliance should be placed on [the magistrate's] findings.'" Nelson v. Smith, 618 F. Supp. 1186, 1189-90 (S.D.N.Y 1985) (internal citations omitted).

IV. ARGUMENT

A. THE SEARCH WARRANT FOR THE DEFENDANT'S RESIDENCE WAS LAWFULLY ISSUED UPON A SHOWING OF SUFFICIENT, RELIABLE, NON-STALE PROBABLE CAUSE

The defendant contests the reliability of the of the information supplied in the application for the search warrant because the foreign law enforcement agency is not identified. *See* Doc. 27-2. Further, the defendant argues the information offered in support of probable cause was "clearly stale and not of a sufficiently recent vintage to allow for a finding of probable cause." *Id.* The government maintains the information presented in the search warrant application was sufficient, reliable, and satisfactorily fresh to support the finding of probable cause. Even if this Court disagrees, the good faith exception should apply. *United States v. Leon*, 468 U.S. 897 (1984).

1. The Information Offered in Support of the Search Warrant Was Sufficient to Justify a Finding of Probable Cause

Probable cause for a search warrant exists when, "given all the circumstances set forth in the affidavit . . . there is a fair probability that contraband or evidence of a crime will be found in a particular place." *Illinois v. Gates*, 462 U.S. 213, 238 (1983). "Probable cause…is not a high bar: It requires only the 'kind of fair probability on which reasonable and prudent people, not legal technicians, act.'" *Kaley v. United States*, 571 U.S. 320, 338 (2014). When reviewing the validity of a search warrant:

> "the duty of [the] court … is simply to ensure that the magistrate had a substantial basis for … conclud[ing] that probable cause existed. A search warrant issued by a neutral and detached magistrate is entitled to substantial deference, and doubts should be resolved in favor of upholding the warrant."

United States v. Rosa, 11 F.3d 315, 326 (2d Cir. 1993) (quotations and citations omitted); *Walczyk v. Rio*, 496 F.3d 139, 157 (2d Cir. 2007) ("[A] reviewing court must accord considerable deference to the probable cause determination of the issuing magistrate…."). "[A]fter-the-fact scrutiny by courts of the sufficiency of an affidavit [applying for a warrant] should not take the form of *de novo* review." *United States v. Smith*, 9 F.3d 1007, 1012 (2d Cir. 1993) (quoting *Gates*, 462 U.S. at 236). "[R]esolution of doubtful or marginal cases in this area should be largely determined by the preference to be accorded to warrants." *Id*. (quoting *United States v. Ventresca*, 380 U.S. 102, 109 (1965)).

Here, the FLA has provided evidence that a particular IP address "was used to access online child sexual abuse and exploitation material" via one of the websites under investigation. The FLA has not provided further information about the particular material that any individual target accessed or downloaded or evidence that the target registered an account on the Target Website. However, 18 U.S.C. § 2252A(a)(5)(b) prohibits the access of a website with the intent to view child pornography. The statute "does not require a showing that [a defendant] actually viewed illegal content on the site." *United States v. Tagg*, 886 F.3d 579, 587 (6th Cir. 2018). In *Tagg*, the Sixth Circuit reversed a trial court's grant of a motion to suppress evidence seized during a court-authorized search of the residence of a target identified as a user of the "Playpen" Tor child pornography hidden service website. In finding that the warrant was amply supported by probable cause, the court opined that "even if the person never viewed illegal child pornography, knowingly accessing a child-pornography website with the intent to view illegal materials is itself a criminal act" so that "probable cause to search [an offender's] house would exist even if he was 'curiosity shopping' for child porn on [the website] but never actually viewed an illegal image." *Id*. at 587-88; *cf. United States v.*

Vosburgh, 602 F.3d 512, 526 (3rd Cir. 2010) (affirming trial court denial of motion to suppress evidence where IP address was tied to attempts to access a link to child pornography; noting that "[a]ttempted possession of child pornography is a federal crime" and therefore evidence of offender's attempts to access a link were "undoubtedly criminal activity.").

There are particular articulable facts contained in the warrant affidavit for this investigation that establish probable cause to believe that, at a minimum, Stuart accessed a Target Website with intent to view child pornography.

First, a target who accesses one of the Target Websites made a purposeful choice to use and access the Tor network. Because Tor hidden services cannot generally be accessed through the traditional internet, only a user who had installed the appropriate Tor software on the user's computer could access one of the websites under investigation. While there are myriad lawful uses of Tor anonymity, an offender's use of Tor to hide his/her identity online while accessing illicit content is some evidence of consciousness of guilt.

Second, a target who accessed one of the Target Websites had to find it. The 16 or 56 character web addresses for Tor hidden services – which consist of a series of semi-random characters – are hard to find without purposefully searching for them. Also, hidden service websites on the Tor Network are not "indexed" by search engines—such as Google—to anywhere near the same degree as websites that operate on the open Internet. Accordingly, it is more difficult to perform a Google-type search of hidden service websites than it is to search open Internet websites for particular content of interest. Users interested in accessing child exploitation material (or in advertising child exploitation and pornography websites they operate) therefore keep, maintain, and use directory sites that advertise the web addresses of hidden services that contain child exploitation related content. Those directory sites also

operate via the Tor network. Users (and law enforcement agents) use those directory sites to identify new web forums, chat sites, image galleries and file hosts pertaining to thening to the sexual exploitation of children. Such directory sites often identify whether particular sites are then operating, whether child pornography imagery may be found there, and even what types of child pornography are accessible (i.e., boys, girls, or "hurtcore"). They also contain clickable hyperlinks to access those sites. As with other hidden service websites, a user must find the 16-or-56 character web address for a directory site in order to access it.

While it operated, the web addresses for the Target Website was listed on one or more of such directory sites advertising hidden services dedicated to the sexual exploitation of children. Accordingly, as articulated in the warrant application, because accessing the Target Website required numerous affirmative steps by the user – to include downloading Tor software, accessing the Tor network, finding the web address for the website, and then connecting to the website via Tor – it is extremely unlikely that any user could simply stumble upon a Target Website without understanding its purpose and content.

Courts have recognized the unique characteristics of Tor child pornography websites and drawn favorable inferences in support of probable cause from them. *See Tagg*, 886 F.3d at 587 (finding it "unlikely" defendant "stumbled upon" the Playpen hidden service "by accident" because "[t]o access the site, he had to obtain the URL from someone 'on the inside' who could provide the exact sequence of numbers and letters to enter into his browser" which "creat[ed] an inference" that the defendant deliberately accessed the website); *United States v. DeFoggi*, 839 F.3d 701, 706–07 (8th Cir. 2016)(upholding denial of probable cause challenge to residential warrant where the warrant affidavit explained that the pertinent Tor child pornograrnography website "could not be accessed without the installation of appropriate

software and knowledge of its exact web address" which a user could find "directly from other users, or from internet postings describing [the website's] content and location;" accessing the website therefore "required numerous affirmative steps by the user, making it extremely unlikely that a user would stumble upon it without knowing that its purpose was to advertise and distribute child pornography and understanding the content to be found there.").

Moreover, the absence of evidence of subscription, membership or download should not defeat probable cause. Courts have assigned weight to other factors pertinent here, to include the website's design and how prominently it displayed images of child pornography. *See Gourde*, 440 F.3d at 1068 (looking to the website's prominent display of nude prepubescent females engaging in sexual acts in considering defendant's intent to access or view child pornography); *Martin*, 426 F.3d at 75-76 (online child pornography trading group's welcome page was titled "girls 12 – 16," which made plain "its essential purpose to trade child pornography"). Here, the welcome page and rules of the Target Website renders it unmistakable in its dedication to illicit child pornography.

Third, review of data seized by the FBI in the Playpen investigation found that it was exceedingly rare for a registered site user to access such a site and never return. "Playpen" was a Tor network-based hidden service dedicated to the advertisement and distribution of child pornography that operated from August 2014 until March 2015. Similar to the Target Website, Playpen was a highly categorized web forum with hundreds of thousands of users that allowed users to post and download messages pertaining to child exploitation within forum categories indexed by the age and gender of child victims and the type of sexual activity involved. In February and March of 2015, the FBI seized and briefly operated the Playpen website for two weeks, using a court-authorized investigative technique to successfully

identify IP addresses and other information associated with site users. FBI review of site data seized from the Playpen website during the operation determined that of over 400,000 total user accounts observed on the Playpen website during its existence, less than 0.02 percent (that is, less than two hundredths of one percent) of user accounts registered an account on the website, accessed a message thread on the website, and then never returned to the site and logged in to the same account. The warrant articulates these findings. *See* 20-MJ-5207 at ¶ 29. While that represents anecdotal data from only one similar website and tracks registered user behavior, that data is useful in supporting probable cause.

Fourth, the agent articulated in the warrant affidavit characteristics that are common to individuals who access with intent to view child pornography – such as the tendency to collect or retain child pornography. *See* 20-MJ-5207 at ¶ 41.

In summary, the Magistrate Judge clearly had a substantial basis to conclude that, given the totality of the circumstances, there was a fair probability of finding evidence that the internet user at the Target IP Address accessed or attempted to access child sexual abuse and exploitation material. The affidavit accurately reiterates the FLA's tip that the internet user at the Target IP Address "was used to access online child sexual abuse and exploitation material via a website that the FLA named and described. 20-MJ-5207 at ¶ 24.

2. <u>The Information Offered in Support of the Search Warrant Was Reliable</u>

The defendant argues the anonymity of the FLA renders its information unreliable and analyzes the issue as though the FLA were an unidentified informant. Such misapprehends the law and is unconvincing in that it is contradicted by established precedent. Indeed, the FLA's information should be considered by this Court as hearsay, not as uncorroborated information supplied by an anonymous civilian informant.

As a general matter, the Supreme Court has made clear that "an affidavit relying on hearsay 'is not to be deemed insufficient on that score, so long as a substantial basis for crediting the hearsay is presented.'" *Gates*, 462 U.S. at 241-42 (citing *Jones v. United States*, 362 U.S. 257, 269 (1960)). In this case, there is more than a substantial basis for crediting the hearsay. As the affidavit established, the FLA is a law enforcement agency that is well-known by the FBI and that has a long history of sharing reliable information with the United States. 20-MJ-5207 at ¶ 24. It is well-established that proven, reliable enforcements generally and law enforcement agencies in particular are entitled to considerable credence. *See Ventresca*, 380 U.S. at 111 (stating that law enforcement officers "are plainly a reliable basis for a warrant applied for…"); *see also Velardi v. Walsh*, 40 F.3d 569 (2d Cir. 1994).

There is no doubt that this presumption of credibility extends to reliable foreign law enforcement agencies like the FLA in tis case. The Third Circuit stated this presumption clearly in *United States v. Benoit* in its affirmance of the Coast Guard's reliance on a tip from Grenadian law enforcement authorities based on the fact that the agency was a known and repeat player in a working relationship with the Coast Guard. *United States v. Benoit*, 730 F.3d 280, 285 (3d Cir. 2013) ("[A] tip from one federal law enforcement agency to another implies a degree of expertise and a shared purpose in stopping illegal activity, because the agency's identity is known."). Given this FLA's history of providing reliable tips to the FBI and this FLA's status as a respected law enforcement agency, it was reasonable for the Magistrate Judge to rely on the FLA tip even if no further corroboration had been done. However, corroboration by the FBI was performed by their own agents visiting the Target Website, collecting observations of its content and features and downloading images of child sexual abuse and exploitation material. *See* 20-MJ-5207 at ¶ 17.

The defendant's enumerated questions posed regarding the FLA's identity and details of its information score points as demonstrative of an interested, curious, inquiring mind – but are nothing more than interesting questions. *See* Doc. 27-2 at p. 4. The law simply does not require the defendant be supplied with that information in discovery, nor does it require the affiant in a search warrant application provide those answers to the issuing magistrate. The FLA source of information is unlike a traditional "confidential informant" in material ways – the FLA is a "member" of law enforcement, it is not under arrest, it is not a drug user, it is not even an "individual" but rather an institution, and as a result it has no apparent reason to manufacture false tips to the United States. The Court should deem the FLA credible and its information reliable, as did the Magistrate Court.

3. <u>The Information Offered in Support of the Search Warrant Was Not Stale</u>

Stuart argues the information presented to Magistrate Judge Michael J. Roemer was stale and could not support the finding of probable cause. *See* Doc. 27-2 at pp. 5-11. The pertinent dates supplied to the Magistrate Judge in the application are the following: (1) on May 28, 2019, the IP address registered to Stuart at his residence was used to access the Target Website on the Tor network with intent to view child pornography; (2) on July 24, 2020 surveillance was conducted at Stuart's residence confirming he was present there; and (3) between August 20, 2020 and October 6, 2020, the PRTT confirmed a user of the internet at Stuart's residence accessed the Tor network on 14 separate dates. *See* 20-MJ-5207 at ¶ 32, 35, 38.

"In determining whether probable cause exists, the magistrate is required to assess whether the information adduced in the application appears to be current, *i.e.*, true at the time of the application, or whether instead it has become stale." *Rivera v. United States*, 928 F.2d

592, 602 (2d Cir. 1991). "The doctrine of staleness applies when information proffered in support of a warrant application is so old that it cases doubt on whether the fruits or evidence of a crime will still be found at a particular location." *United States v. Lamb*, 945 F.Supp.441, 459 (N.D.N.Y. 1996). "While there is no bright line rule for staleness, the facts in an affidavit supporting a search warrant must be sufficiently close in time to the issuance of the warrant and the subsequent search conducted so that probable cause can be said to exist as of the time of the search and not simply as of some time in the past." *United States v. Wagner*, 989 F.2d 69, 75 (2d Cir. 1993). Accordingly, "[t]he information offered in support of the application for a search warrant is not stale if 'there is [a] sufficient basis to believe, based on a continuing patter or other good reasons, that the items to be seized are still on the premises.'" *United States v. Lacy*, 119 F.3d 742, 745-46 (9th Cir. 1997) (quoting *United States v. Gann*, 732 F.2d 714, 722 (9th Cir.), *cert. denied*, 469 U.S. 1034 (1984)), *cert. denied*, 523 U.S. 1101 (1998).

"[T]he principal factors in assessing whether or not the supporting facts have become stale are the age of those facts and the nature of the conduct alleged to have violated the law." *United States v. Diaz*, 176 F.3d 52, 109 (2d Cir.), *cert. denied*, 528 U.S. 875 (1999). "Some types of evidence are more likely to remain in one location than other types of evidence." *United States v. Patt*, 2008 WL 2915433, *12 (W.D.N.Y. 2008). In addition, "[w]here the criminal activity is suspected to be ongoing, 'the passage of time between the last described act and the presentation of the application becomes less significant.'" *United States v. Gayle*, 2009 WL 4667093, *3 (S.D.N.Y. 2009) (quoting *United States v. Gallo*, 863 F.2d 185, 192 (2d Cir. 1988), *cert. denied*, 489 U.S. 1083 (1989)). Accordingly, "[t]he age of the information is relevant only insofar as it affects the likelihood that evidence will be found at the premises." *See United States v. Zoernack*, 2005 WL 1837962, *2 (S.D.N.Y. 2005).

The information contained in the affidavit in support of the application for a search warrant for Stuart's residence was not stale. The investigation confirmed that Stuart was the subscriber of record of the Charter Communications account for the pertinent IP address on the date the Target Website was accessed. Further confirmation that Stuart was still living at the residence was accomplished through surveillance of Stuart himself and his registered vehicle at 1010 Cleveland Drive, Cheektowaga, New York. Although approximately 15 months passed from the date of access of the Target Website on the Tor network to the PRTT, the data revealed by the PRTT confirmed Stuart (or a user from his residence) was still accessing the Tor network on a regular basis. In fact, of the approximately 46 days PRTT data was analyzed between August 20 and October 6, 2020, a user of the internet accessed the Tor network 14 times – that is approximately once every three days. The affiant went on to provide comprehensive details about the means and methods child pornography offenders utilize electronic devices to store images and videos, stating, "[t]he computer's ability to store images in digital form makes the computer itself an ideal repository for child pornography." *See* 20-MJ-5207 at ¶ 40. Further, he detailed the fact that "a computer user's internet activities generally leave traces or 'footprints' in the web cache and history files of the browser used. Such information is often maintained *indefinitely* until overwritten by other data." *Id*. The clear inference one may draw from these facts is that even if Stuart's first and only access of child sexual abuse and exploitation material was the single event in May 2019 when the FLA captured his IP address, there is a high degree of likelihood that forensic evidence of that single access could be found even years later. *See* 20-MJ-5207. This inference was reinforced by the affiant's experience, among a detailed summary, that individuals who access child sexual abuse and exploitation material "typically retain those materials and child erotica for

many years." *See* 20-MJ-5207 at ¶ 41. Further, even if those materials were deleted by the user, the affiant explained that "evidence of such activity, including deleted child pornography, often can be located on these individuals' computers and digital devices through the use of forensic tools." *Id*.

The affiant did not rely on the access date in May 2019 alone, however, because the PRTT confirmed Stuart (or a user from his residence) was accessing the Tor network regularly and as recently as October 6, 2020 – two days prior to the application. Such information, at the very least, confirmed to the Magistrate Court that an individual residing at 1010 Cleveland Drive still had an electronic device capable of connecting to the internet, that they were using the internet, and that they were using the internet to access the Tor network a/k/a "dark web" – the same avenue used by a user in May 2019 to visit the child pornography hub at the Target Website.

The defendant discounts this information by boldly claiming "[t]here is absolutely nothing inherently nefarious about [the Tor network]" and goes on to allege that it is used by "journalists, lawyers, and parents who do not want their children tracked online." *See* Doc. 27-2. Stuart, however, is none of these: journalist, lawyer, nor parent. The affidavit confirmed Stuart was a 32 year-old paramedic with a private ambulance service in Western New York. Stuart is also apparently childless. The fact is that darknet markets operating on the Tor network, which anonymize its users and vendors, clearly function as an effective black market for illicit goods like drugs, firearms, personal identifying information of others, and unsurprisingly, child sexual abuse and exploitation material.[2] The defense asks this Court to

[2] *See e.g.* "More than 400 .Onion Addresses, Including Dozens of 'Dark Market' Sites Targeted as Part of Global Enforcement Action on Tor Network" Dep't of Justice, Nov. 7, 2014, *available at* https://www.justice.gov/opa/pr/more-400-onion-addresses-including-dozens-dark-market-sites-targeted-part-global-enforcement

ignore that fact and require the government to disprove all innocent explanations, even if implausible or demonstrably inapplicable here. "The fact that an innocent explanation may be consistent with the facts alleged…does not negate probable." *United States v. Fama*, 758 F.2d 834, 838 (2d Cir. 1985); *United States v. Delossantos*, 536 F.3d 155, 161 (2d Cir. 2008) ("[W]e cannot discount facts one by one simply because [the defendant] has suggested hypothetical explanations for them that are consistent with his innocence."); *Illinois v. Gates*, 462 U.S. 213, 244 n. 13 (1983) ("innocent behavior frequently will provide the basis for a showing of probable cause; to require otherwise would be to *sub silentio* impose a drastically more rigorous definition of probable cause than the security of our citizens demands.").

This Court should not discount the significance of Stuart's regular and recent accessing the Tor network, especially given the proof that he used it *at least* once in May 2019 to access horrific and clearly unlawful child sexual abuse and exploitation material.

4. Law Enforcement Relied on the Search Warrant in Good Faith and Suppression is Unwarranted

The Fourth Amendment exclusionary rule should not be applied to evidence obtained by a police officer whose reliance on a search warrant issued by a neutral magistrate was based on "objective good faith," even though the warrant itself might ultimately be found to be defective. *See United States v. Leon*, 468 U.S. 897, 926 (1984) (observing "[i]n the absence of an allegation that the magistrate abandoned his detached and neutral role, suppression is appropriate only if the officers were dishonest or reckless in preparing their affidavit or could have not harbored an objectively reasonable belief in the existence of probable cause."); see also, *United States v. Martin*, 157 F.3d 46, 53 (2d Cir. 1998) (holding that because the officers who executed the search warrants acted in good faith, there was no need to suppress evidence thus discovered, even if the search warrant neglected to describe the items to be seized with

particularity or even if the warrant was stale when issued). Even if the magistrate judge lacked a substantial basis for concluding probable cause existed for the search warrant, or that the information was "stale" as the defendant argues, the evidence in this case should not be suppressed because the officers relied in good faith up on a search warrant issued by a neutral and detached judge. The defendant has proffered no reason to believe the affiant in this matter was dishonest or reckless in preparing his affidavit, nor that the Magistrate Judge Michael J. Roemer was anything but neutral and detached. The defendant has failed to identify material false statement, made either knowingly, intentionally, or with reckless disregard for the truth, by law enforcement whatsoever. Accordingly, the rationale of deterrence underlying the remedy of suppression would serve no purpose here. The exclusionary rule "cannot be expected, and should not be applied, to deter objectively reasonable law enforcement activity." *Leon*, 468 U.S. at 919. Accordingly, suppression is unwarranted in this matter.

CONCLUSION

The government respectfully requests that the Court deny Stuart's motion to suppress.

DATED: Buffalo, New York, February 15, 2022

TRINI E. ROSS
United States Attorney

By: ***/s/ LAURA A. HIGGINS***
Assistant United States Attorney
United States Attorney's Office
Western District of New York
138 Delaware Avenue
Buffalo, NY 14202
716/843-5862
Laura.Higgins@usdoj.gov